Introducing BDO & C5 Cyber Security Services:

Protecting organisations in the modern threat landscape.

In an era where cyber threats are increasingly diverse and sophisticated, driven by advancing technology and geopolitical dynamics, businesses must adopt robust cyber security strategies to protect their assets and maintain operational integrity.

The cyber threat environment

EVOLVING DYNAMICS AND DIVERSE ACTORS DRIVE MODERN CYBER CHALLENGES

The cyber threat environment is increasingly complex; a trend driven by advancing technology and the geopolitical environment. Nation states, state-backed actors, activist groups, and criminals exploit vulnerabilities using a range of sophisticated techniques. Cyber crime costs trillions annually, with emerging technologies like AI adding to the challenges.

The cyber threat environment continues to diversify, intensify and proliferate. The change is driven by advancing technology, the geopolitical environment, and an increasingly complex web of threat actors. Cyber capabilities are now a fundamental lever of power for Nation States, used to project influence, acquire information, and advance the national interest.

The geopolitical situation means that states are prepared to use the full spectrum of their capabilities more openly with fewer concerns that activity will be attributed to them. It also means that states are more comfortable providing high-level capabilities to state-backed, but crucially deniable, actors.

Separately, the activist space is growing; entities such as the International Consortium of Investigative Journalists or Bellingcat harness impressive digital forensic, research and data acquisition techniques. Despite this, the most prolific actors remain criminals, both organised and opportunistic. Many are sat beyond the reach of law enforcement, and while most lack sophisticated tools, these actors are capable of building and deploying malware, or conducting cyber-enabled fraud, at scale.

In 2023, the global cost of cyber crime was estimated to reach £8.4 trillion annually, with organised crime groups responsible for a significant proportion of these incidents.

In 2023, the global cost of cybercrime was estimated to reach £8.4 trillion annually.

Collectively, cyber threat actors exploit vulnerabilities in networks and individual devices with a range of well-known and researched tools. Capabilities range from 'denial of service' and 'brute force' attacks, to carefully engineered spear-phishing attacks which use one-click chains to take advantage of misconfigurations, poor policies, ill-equipped people, and social engineering to exploit known vulnerabilities to deploy malware and ransomware.

Beyond this are 'zero-day, zero-click' exploit chains (those where there is no user interaction) against which there is almost no defence. Taking advantage of as yet undisclosed vulnerabilities, these chains allow the most capable and well-resourced threat actors to compromise internet facing devices and networks.

And this is without considering the insider threat, or the unknown, and likely transformative, effect of AI as Large Language Models and Generative Adversarial Networks are brought to bear in the cyber threat space.

Navigating cyber security in the digital economy

ESSENTIAL STRATEGIES FOR ROBUST CYBER DEFENCE

As businesses navigate a complex cyber threat environment, they must prioritise resource to balance security, innovation and accessibility. The need for hybrid working and global connectivity heightens vulnerabilities which can be addressed with a comprehensive cyber security strategy that underpins everyday business operations.

The business need

Set against this complex threat environment, success in the digital and services economy requires speed, innovation, customer experience and delivery – both for clients and employees. Hybrid working (a must for many employees) and the global marketplace require data, services, and infrastructure to be constantly accessible, information easily shareable, and services easily transferable.

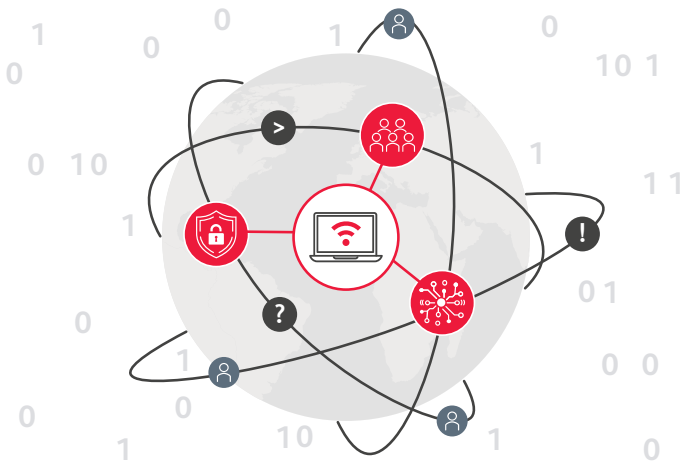
There is also an equally complex cyber defence eco-system from which organisations can mount a response. Security tools, services, training, monitoring, simulation exercises, security operations, incident response and cyber insurance can all be woven together to successfully protect systems, information, and business operations.

Finally, there are regulatory drivers as Governments in the western world seek to harden, protect and secure the cyber environment upon which the global economy depends.

Building a cyber security strategy

Core to any response is developing a cohesive cyber security strategy: designing and implementing an appropriate security architecture, and assuring systems, staff and governance standards.

Understanding the threat environment, your risk profile, the resources available and identifying those critical assets, whether IP, data, or hardware, which need to be protected, is the bedrock of building your strategy to prioritise the expenditure of precious resources.



Safeguarding your business with BDO & C5

Advisory services

We create, refine and implement cyber security strategies for all types of organisation. This includes developing information security policies and robust governance. We deliver workshops and board level briefings on a wide range of topics including the threat environment, regulatory issues and emerging technologies.

We can provide fractional CISOs on a part-time or virtual basis and can deliver organisational threat assessments or risk profiling to help manage information security risks. Security Architecture and Engineering is fundamental to ensure your cyber security is aligned with business objectives and risk tolerance. We advise, design, implement and monitor security controls across infra-structure, endpoints, tools, and data repositories.

Assurance services

We conduct gap analyses and audits against major cyber security frameworks including ISO 27001, C2M2, NIST CSF 2.0, and Cyber Essentials. We conduct cyber maturity assessments and SWIFT attestations, and can act as both an implementation partner and implementation support partner as necessary.

We partner with an array of technical security testing providers who can offer bespoke manual penetration testing as well as automated testing and vulnerability scanning. We are able to provide simulated phishing attacks to train and test staff responsiveness and board level incident response exercises.

Operations

We provide a secure managed service, with endpoint security based on the Microsoft ecosystem and augmented by a 24x7x365 operations team. We work with partners to integrate Security Operations Centre services, additional security tooling, and incident response to suit your needs.

Oliver Farber
Director, Strategic Insight & Cyber Security - BDO
ofarber@bdo.je

May 2025

BDO

www.bdo.je

Our Cyber Security Services

SECURING YOUR CYBER AND INFORMATION SECURITY LANDSCAPE

We advise our clients on the cyber threat environment and how it pertains to their organisation and help them identify vulnerabilities in their current cyber security posture. We work with our clients to transform, assure, and run their cyber and information security governance, systems and strategy, balancing risk mitigation and tolerance with time and resource costs.

We provide tailored cyber security services with a comprehensive service offering across our practice areas, helping clients understand the specific cyber threat environment and identify vulnerabilities in their existing security posture.

Our expert team collaborates with clients to transform and assure their cyber and information security governance, systems, and culture, balancing risk mitigation with time and resource costs.

Advisory

- **Strategy and Governance:** Creation, development, implementation and review of all aspects of an organisational cyber security strategy. Development of information security policies and governance.
- **Fractional CISO:** Provision of a Chief Information Security Officer on a part-time or virtual basis.
- **Workshops and Board Briefing:** Briefs covering the cyber threat environment, regulatory issues, emerging technologies, and incident response scenarios.
- **Security Architecture and Engineering:** Alignment of architecture with business objectives and risk tolerance levels. Advisory services including design assurance, implementation and monitoring of security controls for infrastructure, endpoints, tools, and data.
- **Threat Assessment/Risk Profiling:** Organisational threat assessment and risk profiling services to align cyber defence posture with the threat posed.
- **Training and Awareness:** Training for all levels of an organisation. Includes all staff awareness initiatives, phishing and cyber-enabled fraud training.

Assurance

- **Security Assessment and Framework Compliance:** Gap analysis, implementation, advisory and audit services against major frameworks including ISO 27001, C2M2, NIS2 and NIST Cyber Security Framework 2.0.
- **Assessment, Audit, Attestation and Certification:** Cyber Maturity Assessment, Cyber Essentials Certification and Cyber Assurance Level 2 Certification, SWIFT attestation.
- **Cyber Security Testing and Evaluation:** Technical security testing, including automated, regular, and continuous penetration and vulnerability assessments. Simulated phishing attacks to train and test staff responsiveness. Board-level incident response exercises.

Operations

- **Secure IT Service:** Secure infrastructure, architecture, applications, data, and endpoint security based on the Microsoft Ecosystem, augmented by a 24x7x365 operations team.
- **Cyber Security Monitoring:** 24x7x365 service desk and a Security Operations Centre Partner.
- **Security Tooling:** Selection, integration, and oversight of cyber security tools.
- **Cyber Security Incident Response:** Immediate action to contain damage and manage notification responsibilities as jurisdictional experts. Incident response, including digital forensics provided by specialist partners as required.

Contact us

START YOUR CYBER SECURITY JOURNEY WITH BDO & C5

BDO Jersey and C5 Alliance are part of the Windward Group which delivers advisory, assurance and technology services.

Our Cyber Security Services draw from all of our core practices to support organisations to meet the challenges of an evolving cyber threat landscape. Initiating a conversation is the first step toward strengthening your organisation's cyber security.

The team at BDO and C5 is eager to share their insights and expertise, guiding you through your cyber security transformation journey and helping you thrive.

If you would like to learn more about how our cyber security services can fortify your business, please reach out to our team.

Mark McLachlan
Director,
IT Services - C5 Alliance
mark.mclachlan@c5alliance.com

Arthur Mainja
Principle Consultant,
Cyber Security - BDO
amainja@bdo.je

BDO

www.bdo.je